Notice of Allowability	**Application No.** 10/629,292	**Applicant(s)** CHRISTODORESCU ET AL.	
	Examiner SHEWAYE GELAGAY	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/13/09*.

2. ☒ The allowed claim(s) is/are *1-3,6-10 and 12-17*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) □ All b) □ Some* c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *1/25/10* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

DETAILED ACTION

1. This office action is in response to the amendment filed on November 13, 2009.

2. Claims 1 and 12-13 have been amended.

3. Claims 1-10 and 12-17 are pending.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Keith M. Baxter (Reg. No. 31,233) on 01/25/10.

The application has been amended as follows:

In the claims:

Please cancel claims 4 and 5.

With respect to claim 1:

A computer program stored on a computer readable hardware storage medium for identifying malicious portions in a suspect computer program comprising:

a preprocessor portion for receiving the suspect computer program in executable form and creating a logically equivalent standardized version also in executable form of the suspect program without executing the suspect program, the logical equivalent standardized version if executed providing an equivalent result as execution of the suspect computer program;

a library of standardized malicious code portions; and

a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is present in the suspect program

wherein the standardized version maps instructions of the suspect program to corresponding standard synonym instructions; and

wherein the standard synonym instructions are different in number from the instructions of the suspect program to which the synonym instructions map.

With respect to claim 12:

A computer program stored on a computer readable hardware storage medium for identifying malicious portions in a suspect computer program comprising:

a preprocessor portion for receiving the suspect computer program and creating a logically equivalent standardized version of the suspect program without executing the suspect program;

a library of standardized malicious code portions; and

a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is present in the suspect program;

the computer program further including a library of patterns matching to one or more instructions of the suspect program and wherein the preprocessor creates the standardized version by replacing instructions of the suspect program with matching patterns from ~~ones of~~ the library of patterns and wherein the library of standardized malicious code portions are also ~~collections of ones~~ patterns of the library of patterns

wherein a pattern is at least one instruction logically replacing at least one different instruction in the suspect program.

With respect to claim 13:

A computer program stored on a computer readable hardware storage medium for identifying malicious portions in a suspect computer program comprising:

a preprocessor portion for receiving the suspect computer program and creating a logically equivalent standardized version of the suspect program without executing the suspect program;

a library of standardized malicious code portions; and

a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is present in the suspect program;

the computer program further including a library of patterns matching to one or more instructions of the suspect program and wherein the preprocessor creates the standardized version by replacing instructions of the suspect program with matching ~~ones of~~ patterns from the library of patterns and wherein the library of standardized malicious code portions are also collections of ~~ones of~~ patterns from the library of patterns wherein a pattern is a tag replacing at least one instruction logically having no substantive effect on the execution of the suspect program; and wherein the library of patterns is implemented as a look-up table matching instructions to the patterns.

Allowable Subject Matter

4. Claims 1-3, 6-10, 12-17 are allowed.

5. The following is an examiner's statement of reasons for allowance: The prior art on record Nachenberg (US 6,357,008) teaches a method of detecting computer viruses comprising three stages: a decryption phase, an exploration phase and an evaluation phase. A purpose of the decryption phase is to emulate sufficient number of instructions to allow an encrypted virus to decrypt its viral body. Nachenberg (US 6,851,057) teaches a virus detection system (VDS) for detecting the presence of a virus in a file having multiple entry points. The VDS includes a data file holding P-code instructions and a virus definition file containing virus signatures of known viruses. And a scanning module for scanning the memory addresses within the supplied range for signatures held in the virus definition file. An emulating module for setting up a virtual machine having a virtual preprocessor and an associated memory. The virtual machine uses the virtual preprocessor to execute code in the virtual memory in isolation from the reminder of the computer system. Schmall (US 7,069,589) teaches a method of detecting a class of viral code and a heuristic analyzer that analyzes the subject file and generates a set of lags along with statistical information. A search component that uses a set of flags with statistical information to perform a search for a scan string and/or a statement type in the subject file. A positive detection alarm is triggered if the scan string and/or statement is found at least a corresponding predetermined number times.

6. **With respect to claim 1**:

The prior art on record either taken singularly or in combination fails to teach the identifying malicious portion in a program specifically "***a preprocessor portion creating a logically equivalent standardized version also in executable form of the suspect program without executing the suspect program, the logical equivalent standardized version if executed providing an equivalent result as execution of the suspect computer program; a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is present in the suspect program wherein the standardized version maps instructions of the suspect program to corresponding standard synonym instructions; and wherein the standard synonym instructions are different in number from the instructions of the suspect program to which the synonym instructions map***" including all the other limitations recited in the independent claim 1.

With respect to claim 12:

The prior art on record either taken singularly or in combination fails to teach the identifying malicious portion in a program specifically "***a preprocessor portion for receiving the suspect computer program and creating a logically equivalent standardized version of the suspect program without executing the suspect program; a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is present in the suspect program; and wherein the***

preprocessor creates the standardized version by replacing instructions of the suspect program with matching patterns from library of patterns and wherein the library of standardized malicious code portions are also patterns of the library of patterns wherein a pattern is at least one instruction logically replacing at least one different instruction in the suspect program" including all the other limitations recited in the independent claim 12.

With respect to claim 13:

The prior art on record either taken singularly or in combination fails to teach the identifying malicious portion in a program specifically "***a preprocessor portion for receiving the suspect computer program and creating a logically equivalent standardized version of the suspect program without executing the suspect program; a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is present in the suspect program; wherein the preprocessor creates the standardized version by replacing instructions of the suspect program with matching patterns from the library of patterns and wherein the library of standardized malicious code portions are also collections of patterns from the library of patterns wherein a pattern is a tag replacing at least one instruction logically having no substantive effect on the execution of the suspect program; and wherein the library of patterns is implemented as a look-up table matching instructions to the patterns***." including all the other limitations recited in the independent claim 13.

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Shewaye Gelagay/
Examiner, Art Unit 2437

/Michael Pyzocha/
Primary Examiner, Art Unit 2437